

ABSTRACT OF THE DISCLOSURE

The present invention relates to a device (1) comprising an input for receiving an input; calculation means (P) for producing a response (OUTPUT) in response to the input (INPUT) and a secret key (A) by utilizing a first predetermined function (f), and an output (3) for feeding
5 said response (OUTPUT) further. In order for an attacker not be able to find out the secret key, the device further comprises a memory (M) in which the key-specific number (RND) is stored, and means for retrieving the key-specific number (RND) from the memory (M) and for feeding it to the calculation means (P') for carrying out predetermined calculation operations (f2) on the basis of the key-specific number (RND) when producing said response (OUTPUT).